Computer Security in the Age of the Internet

By

Timothy E. Reardon
Defense Institute of Security Assistance Management

Computer security prior to the internet was relatively easy. Few organizations had the capability to access computer systems outside of their organization. There was little chance that those computer systems that did have access outside the organization could be infected with a computer virus. The arrival of the internet provides easy access to and rapid dissemination of information from a variety of sources, http://www.asc.wpafb.af.mil/cbt/content/iabasics/slide30.html. The key now is to provide users with maximum internet availability; when using computer systems for performing official organizational business, while safeguarding against security risks. This article will provide insights concerning establishing a computer security program.

The term information assurance is used by government agencies in addition to the term "computer security". The components of information assurance are that only authorized users have access to systems http://ase50.wpafb.af.mil/cbt/content/iabasics, that these computer systems operate correctly and the data provided by these computer systems is accurate. Information assurance is not a program, but the integration of people, policy, technology, procedures and doctrine.

As we evaluate computer security in our organizations, it is important to look at identifying computer system vulnerabilities and correcting these vulnerabilities. This is known as risk management. We will look at risk management, the physical and software aspects of computer security, and computer security tools users and organizations can use in identifying and eliminating securities vulnerabilities.

Risk Management

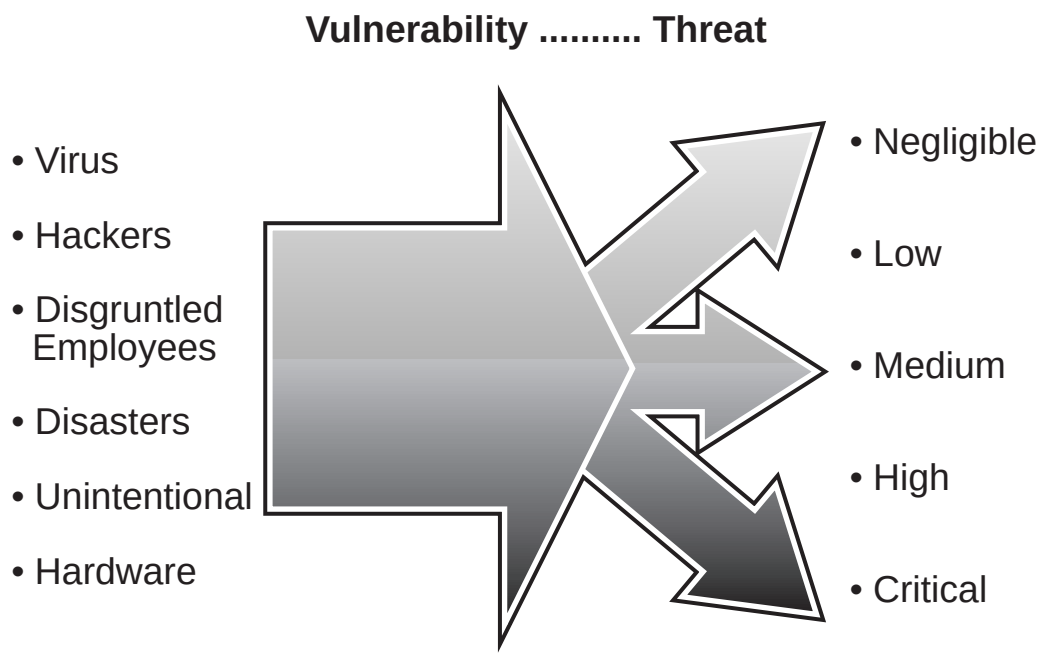
A fundamental aspect of risk management is the identification of vulnerabilities and their associated threats. The chart on the next page identifies the different types of vulnerabilities and the threat levels associated with these vulnerabilities. An example of this is viruses. All viruses attack potential system vulnerabilities; however, the associated risk with a particular virus can be low, medium, or high depending on the damage that can be done. You should also realize that computer systems are not just subject to vulnerabilities which are intentionally inflicted by hackers or disgruntled employees but may result from natural disasters, such as floods or fires. In addition, there are also unintentional vulnerabilities, such as a employee mistakenly deleting an important file needed by the organization.

Computer Security

The most important elements of computer security are physical security, security provided by the operating system the computer system uses, computer security software applications and encryption, and combinations of both physical and security software applications .

Physical security relates to the physical barriers that may be in place to prevent unauthorized access to computers. Doors, dead bolts, and key control systems are example of physical security devices for facilities.

The operating system that the computer system uses to process commands or instructions also has built-in security features, such as password protection for user accounts and screen savers.



Hackers, however, have discovered vulnerabilities in the operating system software, especially computer systems that are used as web servers, and they have exploited these vulnerabilities to gain unauthorized access to computer systems. Microsoft and other operating system software developers continuously provide software releases to correct these vulnerabilities. The reader should be aware of which operating system software is being used on your computer system and should ensure that the latest service releases are installed.

Software applications such as Norton or McAffee anti-virus products are examples of computer security software applications. Additionally, software used in enabling public key and other encryption technologies are also examples of computer security software applications.

Firewall and proxy servers can use both physical hardware and software to protect computer users. A firewall protects all computer systems within a defined boundary and allows only authorized users outside the boundary to access computer systems within the boundary; users not listed in the firewall server's access list are excluded from computer systems within the boundary. Think of a computer firewall in the same regards as a car firewall. A firewall in a car is designed to protect the occupants of the car from injury by preventing the spread of an engine fire to the driver and passenger compartments of the car. A computer firewall protects computer systems within the designated boundary and prevents access to these systems by unauthorized users.

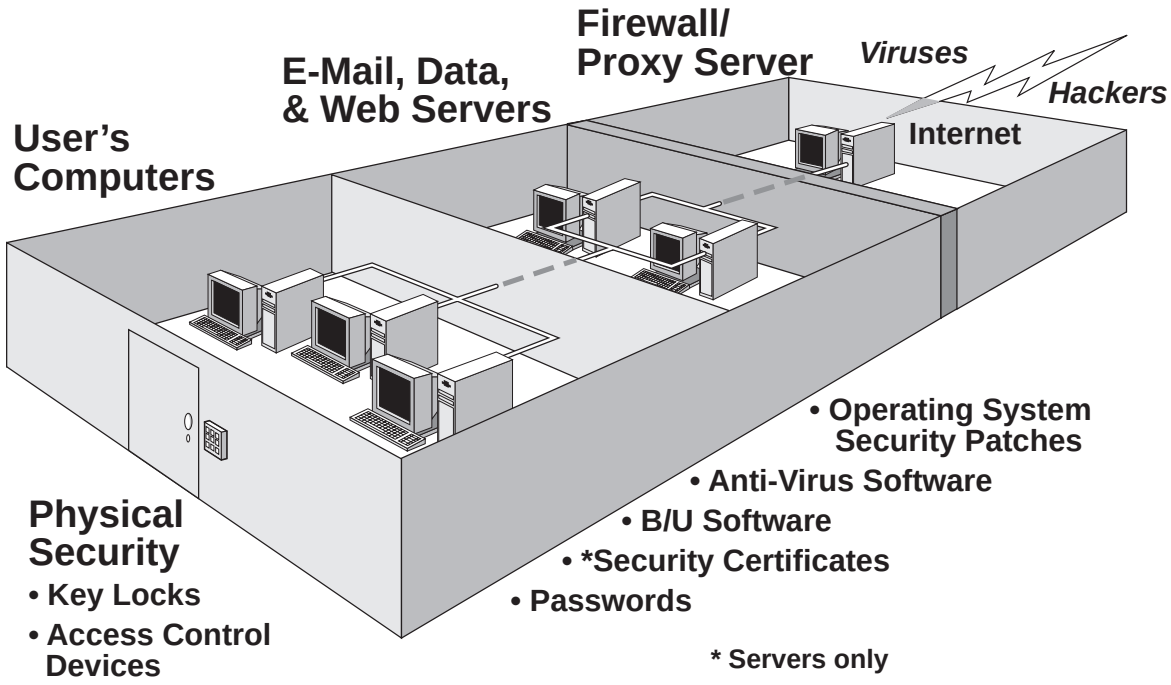
A proxy server is slightly different from a firewall in that a proxy server does not allow direct access to an authorized computer system. Instead, a proxy server is used in conjunction with web servers to retrieve pages a user requests. When a user attempts to access the web server, the proxy server intercepts the request. The proxy server then requests the pages from the web server and sends the requested pages to the user. The user in this case never accesses the web server directly; however, the user does receive the requested information. This processes ensures that users cannot connect to the web server and introduce computer viruses or malicious code to the web server.

Computer Security Tools

A virus is a self-replicating, malicious program introduced to computer systems and leaves no obvious signs of its presence. A virus can destroy all the data on your hard drive and leave the

drive inoperable. The four steps to virus protection are to prevent viruses, detect viruses, eradicate viruses, and to report virus incidents. Computers system that display the following signs could be infected with a computer virus:

- Unable to operate
- Unusual messages displayed
- Files are missing, have increased in size, or are corrupt
- System operates slowly
- Sudden lack of disk space
- Unable to save or access a file



Example of a computer security system

The most important security tool is virus protection software. Make sure it is installed on your computer system and make sure you have the most current virus definitions. Virus definitions are updated when new viruses discovered. The virus definition files are released whenever necessary to combat against new known viruses, so it is important that the current virus definition file is installed on your computer system. You need to remember that a virus definition may not have been released for a computer virus that was recently discovered. Thus the battle to create new definitions is never ending. You have to wait until the anti-virus manufacturer has found a cure for the virus and released a new virus definition file.

Other computer security tools are monitoring event logs on servers, ensuring that file and account permissions are properly set, that computer systems use password protection and that

passwords are composed of at least eight characters and that the password combination includes both letters and numbers (alphanumeric) and has at least one special character.

Physical security is also very important and should not be overlooked. Access should be limited to the area where the network servers and communications equipment (network hubs, switches, routers, etc.) are kept. Individuals who depart the organization should no longer have unescorted access to the building or to the computer systems in the building.

Summary

It was indicated at the beginning of this article that the internet provides us with instant access to a vast amount of data; however, it has created security vulnerabilities. The following table is a visual representation of some computer security elements you should consider when implementing a computer security program.

In conclusion, you should remember that if you can see other computer systems on the internet, then users of those computer systems can see or even access your computer system as well. An effective computer security program is designed around the concept of identifying computer vulnerabilities and providing computer system users with guidance on how to eliminate, or at least reduce, these vulnerabilities.

About the Author

Timothy Reardon is an assistant professor at DISAM and has served on the DISAM faculty for ten years. He is the functional manager for the DISAM network and is the organization's computer security officer. Timothy has designed and installed local area networks for several security assistance field activities and has over seventeen years of computer networking experience. Timothy graduated from Park college with a B.S. in management. He is also an adjunct faculty member of Miami Jacobs College. You may contact Tim at DSN 785-8524, or (937)-255-8524, or by e-mail timothy.reardon@disam.dsca.osd.mil.